

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A trusted sensor (14) for authentication of biometric information used in an encryption system, said trusted sensor (14) disposed on at least one integrated circuit and comprising:

- a microprocessor (34);

- a data memory (36) coupled to said microprocessor (34) and configured to hold

- a plurality of templates representing enrolled biometric information, a biometric public key private key pair corresponding to each of said plurality of templates, and a manufacturer public key and private key pair;
 - and

- a functions section (32) coupled to said microprocessor (34), said functions section comprising:

- a cryptographic library module (60) storing one or more public key private key encryption functions and further storing instructions for causing said microprocessor (34) to populate said biometric public key and private key pair corresponding to each of said plurality of templates;

- a feature extraction and template matching module (58) storing instructions for causing said microprocessor (34) to extract features created with a biometric image capture device (24) coupled to said trusted sensor (14) and to populate to at least one of said plurality of templates, and further storing instructions for causing said microprocessor (34) to match sensed biometric information, communicated from said biometric image capture device (24) to said enrolled biometric information stored in said data memory (36) and, based on said match, select a particular biometric private key; and

- an authentication module (56) storing instructions for causing said

microprocessor (34) to certify said trusted sensor (14) to a host computer by executing said one or more encryption functions stored in said cryptographic module (60) using said manufacturer private key and a host computer public key.

2. (Currently Amended) The trusted sensor of claim 1, said authentication module (56) further storing instructions for causing said microprocessor (34) to execute said one or more encryption functions stored in said cryptographic library module (60) using said particular biometric private key, a public key corresponding to a remote computer, said one or more encryption functions encrypting a message destined for said remote computer.

3. (Currently Amended) The trusted sensor of claim 2:

wherein said biometric image capture device (24) includes a plurality of capacitive fingerprint sensing elements; and

wherein said manufacturer public key and private key pair correspond to said plurality of capacitive fingerprint sensing elements.

4. (Currently Amended) The trusted sensor of claim 2:

wherein said biometric image capture device (24) includes a plurality of capacitive fingerprint sensing elements; and

wherein said manufacturer public key and private key pair correspond to said functions section (32).

5. (Currently Amended) The trusted sensor of claims 3, said functions section further comprising;

a power on self-test and tamper detect feature (62) storing instructions for causing said microprocessor (34) to enable said trusted sensor (14) when said power on self-test is successful and said tamper detected feature detects no tampering;

a secure time stamp module (52) storing instructions for causing said microprocessor (34) to generate a time stamp used by said authentication module (56); and

a peripheral interface (50) configured to communicatively couple

microprocessor (50) to said host computer over a secure communications link (46).

6. (Currently Amended) A method for authenticating the identity of an individual in a transaction using a trusted sensor (14), the method of comprising:

- performing a power on self-test on said trusted sensor (14);
- verifying said trusted sensor (14) to a host computer (12) coupled to said trusted sensor (14), said step of verifying using a manufacturer private key (40) and a host computer public key (42);

- receiving biometric information from an image capture device (24);
- determining whether said biometric information from said image capture device (24) matches an enrolled biometric template (26) stored in said trusted sensor (14);

- when the biometric information from said image capture device (24) does match said enrolled biometric template (26) stored in said trusted sensor (14), then:

- selecting a public key (28) and private key (30) pair corresponding to said enrolled biometric template (26), said public key (28) and private key (30) pair stored in said trusted sensor (14);

- receiving a message from said host computer (12), said message including a remote computer public key (46);

- encrypting at least a portion of said message using said selected private key (30) and said remote computer public key (46); and

- sending said encrypted message from said trusted sensor (14) to said host computer (12); however,

- when the biometric information from said image capture device (24) does not match said enrolled biometric template (26) stored in said trusted sensor (14), then deny access to the key pairs and cryptographic library module (60).

7. (Currently Amended) The method of claim 6, said step of verifying comprising;

- receiving an encrypted random number from said host computer (12), said encrypted random number encrypted by said host computer (12) using a host computer private key (44) and a manufacturer public key (38);

decrypting said encrypted random number into a random number using said host computer public key (42) and said manufacturer private key (40);
modifying said random number;
encrypting said modified random number using said manufacturer private key (40) and said host computer public key (42); and
sending said encrypted modified random number to said host computer (42).

8. (Currently Amended) The method of claim 7, further comprising steps preformed by said host computer (42), said steps comprising:

generating said random number;
encrypting said random number using said host computer private key (44) and said manufacturer public key (38) to form said encrypted random number;
sending said encrypted random number to said trusted sensor (14);
receiving said encrypted modified random number from said trusted sensor (14);
decrypting said encrypted modified random number using said host computer private key (44) and said manufacturer public key (38); and
verifying said modification performed by said trusted sensor (14) to said random number.

9. (Currently Amended) The method of claim 8, further comprising steps performed by a said remote computer (20), said steps comprising:

encrypting a primary message with a remote computer private key (48) and a transaction public key, said transaction public key selected from a group comprising said host computer public key (42) and said selected public key (28);
receiving a confirmation message from said host computer (12), said confirmation message comprising said portion of said message encrypted at said trusted sensor (14) using said selected private key (30) and said remote computer public key (46); and
decrypting said portion of said confirmation message using said selected transaction key and said remote computer private key (48).

10. (Currently Amended) A computer software product having stored therein one or more sequences of instructions for causing one or more microprocessors to perform the

steps described in ~~any of above claims~~ claim 6 through ~~9~~.

11. (Currently Amended) A high security biometric authentication system (10) using public key private key pairs comprising:

- a remote computer (20) including a remote computer public key (46) and private key (48) pair;

- a host computer (12) coupled to said remote computer (20), said host computer (12) including a host computer public key (42) and private key (44) pair;

- a biometric image sensing means (24) including a plurality of capacitive sensing elements for measuring relative distances between ridges and valleys on a fingerprint; and

- a trusted sensor (14) coupled to said biometric image sensing means (24) and said host computer (12), said trusted sensor (14) including a microprocessor (34), and a data memory (36) including a plurality of biometric templates (26), each of said plurality of biometric templates (26) having a biometric template public key (28) and private key (30) pair and a manufacturer public key (38) and private key (40) pair, said plurality of biometric templates (26) comprising manipulated biometric information sensed by said biometric image sensing means (24), and said trusted sensor (14) further including a functions section (32) accessible by said microprocessor (34), said functions section (32) comprising a feature extraction and template matching module (58) comprising instructions for causing said microprocessor (34) to compare biometric information sensed by said biometric sensing means (24) to one or more of said plurality of biometric templates (26) and further comprising instructions to select biometric template private key (30) only if a match is found.

12. (Currently Amended) The high security biometric authentication system (10) of claim 11, wherein said trusted sensor (14) is verified by host computer (12) by:

- sending a first message from said host computer (12) to said trusted sensor (14), said first message encrypted with said host computer private key (44) and

- said manufacturer public key (38);

- receiving said first message at said trusted sensor (14), decrypting said first

message, manipulating a portion of said first message, returning a return first message to said host computer (12), said return first message including said manipulated portion of said first message and said return first message encrypted with said manufacturer private key (40) and said host computer public key (42); and

receiving said return first message from said trusted sensor (44) at said host computer (12), decrypting said return first message with said host computer private key (44) and said manufacturer public key (38) and verifying said manipulation to said portion of said first message.

13. (Currently Amended) The high security biometric authentication system (40) of claim 12, wherein a transaction is verified, after first verifying said trusted sensor (44), by:

sensing current user biometric information using said biometric image sensing means (24);

comparing said current user biometric information to said plurality of biometric templates (26);

selecting a particular biometric image template that matches said current user biometric information, said act of selecting including identifying a particular biometric public key and private key pair corresponding to said particular biometric image template;

encrypting a second message authorizing a transaction with said particular biometric private key and said remote computer public key (46);

sending said second message to said host computer (12);

receiving said second message from said trusted sensor (44) at said host computer (12);

re-transmitting said second message from host computer (12) to said remote computer (20);

receiving said re-transmitted second message from host computer (12) at said remote computer (20); and

verifying said re-transmitted second message using said host computer private key (48) and said particular biometric public key.

14. (Currently Amended) The high security biometric authentication system (40) of

claim 13:

wherein prior to said step of re-transmitting said second message, said host computer encrypts said second message using said host computer private key (44) and said remote computer public key (46); and
wherein said step of verifying said re-transmitted second message includes verifying said second message using said host computer public key (42).

15. (New) The computer software product of claim 10, wherein said step of verifying comprises:

receiving an encrypted random number from said host computer, said encrypted random number encrypted by said host computer using a host computer private key and a manufacturer public key;
decrypting said encrypted random number into a random number using said host computer public key and said manufacturer private key;
modifying said random number;
encrypting said modified random number using said manufacturer private key and said host computer public key; and
sending said encrypted modified random number to said host computer.

16. (New) The computer software product of claim 15, comprising a first set of instructions causing a host computer to:

generate said random number;
encrypt said random number using said host computer private key and said manufacturer public key to form said encrypted random number;
send said encrypted random number to said trusted sensor;
receive said encrypted modified random number from said trusted sensor;
decrypt said encrypted modified random number using said host computer private key and said manufacturer public key; and
verifying said modification performed by said trusted sensor to said random number.

17. (New) The method of claim 16, further comprising a second set of instructions causing a remote computer to:

encrypt a primary message with a remote computer private key and a

transaction public key, said transaction public key selected from a group comprising said host computer public key and said selected public key; receive a confirmation message from said host computer, said confirmation message comprising said portion of said message encrypted at said trusted sensor using said selected private key (30) and said remote computer public key; and
decrypt said portion of said confirmation message using said selected transaction key and said remote computer private key.

18. (New) A trusted sensor for authentication of biometric information used in an encryption system, comprising:

a microprocessor; and

a data memory coupled to said microprocessor, wherein the data memory is configured to hold a plurality of templates representing enrolled biometric information, a biometric public key private key pair corresponding to each of said plurality of templates, and a manufacturer public key and private key pair.